

CLAIMS

1 1. A method of remotely controlling a security element of a mobile terminal for
2 disabling and enabling access to secured functions of the mobile terminal, the
3 method comprising:

4 receiving a request from a user;

5 verifying authenticity of the user;

6 creating a signed push message including, at least, an address for the
7 mobile terminal and content which causes a disablement application to be
8 executed; and

9 sending the signed push message to the mobile terminal.

1 2. The method of claim 1 wherein the request and the push message are for
2 disabling access, and further comprising:

3 receiving a confirmation message from the mobile terminal; and

4 sending a response message to the user based on the confirmation
5 message.

1 3. The method of claim 1 wherein the request from the user and the push
2 message are for disabling access, and further comprising:

3 determining that the mobile terminal is unavailable; and

4 sending a response message to the user based on a determination that
5 the mobile terminal is unavailable.

09878456-061101

1 4. The method of claim 2 wherein the confirmation message from the mobile
2 terminal is signed.

1 5. The method of claim 4 wherein the confirmation message and the re-
2 sponse include position information for the mobile terminal.

1 6. The method of claim 1 wherein the request and the push message are for
2 enabling access, and further comprising:
3 receiving a confirmation message from the mobile terminal; and
4 sending a response message to the user based on the confirmation
5 message.

1 7. The method of claim 1 wherein the content comprises an identification of
2 an application that resides in the mobile terminal.

1 8. The method of claim 1 wherein the content comprises an identification of a
2 calling program residing at a server.

09373463.061101

1 15. The method of claim 5 wherein the content comprises an identification of
2 an application that resides in the mobile terminal.

1 16. The method of claim 5 wherein the content comprises an identification of
2 a calling program residing at a server.

1 17. The method of claim 6 wherein the content comprises an identification of
2 an application that resides in the mobile terminal.

1 18. The method of claim 6 wherein the content comprises an identification of
2 a calling program residing at a server.

1 19. Apparatus for remotely controlling a security element of a mobile terminal
2 for disabling and enabling access to functions of the mobile terminal, the apparatus
3 comprising:

4 means for receiving a request from a user;

5 means for verifying authenticity of the user;

6 means for creating a signed push message including, at least, an ad-
7 dress for the mobile terminal and content which causes a disablement appli-
8 cation to be executed;

9 means for sending the signed push message to the mobile terminal;

10 means for receiving a confirmation message from the mobile terminal;
11 and
12 means for sending a response to the user based the confirmation mes-
13 sage.

1 20. A computer program product for enabling a computer system to remotely
2 control a security element of a mobile terminal for disabling and enabling access to
3 secured functions of the mobile terminal, the computer program product including a
4 computer program comprising:
5 instructions for receiving a request from a user;
6 instructions for verifying authenticity of the user;
7 instructions for creating a signed push message including, at least, an
8 address for the mobile terminal and content which causes a disablement ap-
9 plication to be executed;
10 instructions for sending the signed push message to the mobile termi-
11 nal; and
12 instructions for sending a response to the user based on an outcome of
13 the sending of the signed push message.

1 21. The computer program product of claim 20 wherein the content comprises
2 an identification of an application that resides in the mobile terminal.

instructions for including the position information for the mobile terminal
in the response.

26. A programmed computer system operable for controlling a security element of a mobile terminal for disabling and enabling access to secured functions of the mobile terminal by performing a method comprising:

receiving a request from a user;
verifying authenticity of the user;
creating a signed push message including, at least, an address for the mobile terminal and content which causes a disablement application to be executed;
sending the signed push message to the mobile terminal; and
sending a response to the user based on an outcome of the sending of the signed push message.

27. The computer system of claim 26 wherein the content comprises an identification of an application that resides in the mobile terminal.

28. The computer system of claim 26 wherein the content comprises an identification of a calling program residing at a server.

1 29. The computer system of claim 26 further enabled to:

2 receive position information for the mobile terminal within a signed
3 confirmation message from the mobile terminal when the request and the
4 signed push message are for disabling access; and
5 include the position information for the mobile terminal in the response.

1 30. The computer system of claim 27 further enabled to:

2 receive position information for the mobile terminal within a signed
3 confirmation message from the mobile terminal when the request and the
4 signed push message are for disabling access; and
5 include the position information for the mobile terminal in the response.

1 31. The computer system of claim 28 further enabled to:

2 receive position information for the mobile terminal within a signed
3 confirmation message from the mobile terminal when the request and the
4 signed push message are for disabling access; and
5 include the position information for the mobile terminal in the response.
6

1 32. A system for controlling a security element of a mobile terminal for dis-
2 abling and enabling access to secured functions of the mobile terminal, the system
3 comprising:

a push initiator operable to create and send signed push messages including, at least, an address for the mobile terminal and content which causes a disablement application to be executed;

a proxy gateway operable to receive the signed push messages and send over-the-air messages to the mobile terminal corresponding to the signed push messages; and

a network interconnecting the push initiator and the proxy gateway.

33. A mobile terminal comprising:

a radio block;

a security element encoded with at least one security key for securing transactions; and

a processor system operably connected to the radio block and the security element, the processor system further operable to disable and enable access to the key in response to unsolicited, over-the-air messages received through the radio block.

34. The mobile terminal of claim 33 wherein the processor system is further operable to disable access to the at least one security key while permitting operations of the security element for which user authentication and authorization services are not required.

35. The mobile terminal of claim 33 wherein the processor system disables access to the at least one security key by disabling access to the security element.

36. The mobile terminal of claim 34 wherein the security element further comprises at least one status register associated with the at least one security key, and wherein the processor system enables and disables access to the key by alternatively setting the status register to a first state wherein access to the at least one security key is enabled and a second state wherein access to the at least one security key is disabled, respectively.

37. The mobile terminal of claim 33 further comprising a global positioning system (GPS) subsystem, and wherein the processor system is further enabled to cause the mobile terminal to send a confirmation message through the radio block, the confirmation message including position information for the mobile terminal, the position information being retrieved from the GPS subsystem.

38. The mobile terminal of claim 34 further comprising a global positioning system (GPS) subsystem, and wherein the processor system is further enabled to cause the mobile terminal to send a confirmation message through the radio block, the confirmation message including position information for the mobile terminal, the position information being retrieved from the GPS subsystem.

1 39. The mobile terminal of claim 36 further comprising a global positioning
2 system (GPS) subsystem, wherein the processor system is further enabled to cause
3 the mobile terminal to send a confirmation message through the radio block, the
4 confirmation message including position information for the mobile terminal, the po-
5 sition information being retrieved from the GPS subsystem.

1 40. A security element for a mobile terminal, the security element encoded
2 with a data structure for providing user authentication services, the data structure
3 comprising:

4 at least one key for securing at least some transactions initiated by a
5 user of the mobile terminal; and

6 at least one status indicator associated with the at least one key, the
7 status indicator settable by the mobile terminal alternatively to a first state
8 wherein access to the at least one key is enabled and a second state wherein
9 access to the at least one key is disabled.

1 41. The security element of claim 40 wherein the at least one key is a plural-
2 ity of key pairs providing user authentication and authorization services through the
3 use of digital signatures, and wherein the at least one status indicator is a plurality of
4 status indicators, further wherein each status indicator is associated with one key
5 pair.

1 42. In a mobile terminal, a method of controlling access to a security key in a
2 security element, the method comprising:

3 receiving an unsolicited, over-the-air request to disable access to the
4 security key in the security element;

5 updating a status register in the security element to disable access to
6 the security key; and

7 sending an over-the-air, secured confirmation message indicating suc-
8 cess of disabling access to the security key.

1 43. The method of claim 42 further comprising:

2 receiving an unsolicited, over-the-air request to re-enable access to the
3 security key in the security element; and

4 updating a status register in the security element to re-enable access
5 to the security key.

1 44. The method of claim 42 wherein the unsolicited over-the-air, request to
2 disable access takes the form of a wireless application protocol (WAP) push mes-
3 sage.

09673456 051101

7 access to the key in response to unsolicited, over-the-air messages received
8 through the radio block.

1 48. The mobile terminal of claim 47 wherein the processor system is further
2 operable to disable access to the at least one security key while permitting opera-
3 tions of the security element for which user authentication and authorization services
4 are not required.

1 49. The mobile terminal of claim 47 wherein the processor system disables
2 access to the at least one security key by disabling access to the security element.

1 50. The mobile terminal of claim 47 further comprising a global positioning
2 system (GPS) subsystem, and wherein the processor system is further enabled to
3 cause the mobile terminal to send a confirmation message through the radio block,
4 the confirmation message including position information for the mobile terminal, the
5 position information being retrieved from the GPS subsystem.

1 51. The mobile terminal of claim 48 further comprising a global positioning
2 system (GPS) subsystem, and wherein the processor system is further enabled to
3 cause the mobile terminal to send a confirmation message through the radio block,

- 4 the confirmation message including position information for the mobile terminal, the
- 5 position information being retrieved from the GPS subsystem.

09078458-061101
FOI b7E b7C b7D